Fingerprint Recognition Using a Transfer Learning Method

Abdoul K. Assouma[1], Tahirou Djara[1], Max F. O. Sanya[1], Abdou-Aziz Sobabe[1]
Blaise Blochaou[2]
[1]*Laboratoire d'Electronique de Télécommunication et d'Informatique Appliquée (LETIA) Université d'Abomey-Calavi (UAC), Benin*
[2]*Institut d'Innovation Technologique (IITECH) Abomey-Calavi, Bénin*

Abstract

Individuals' recognition has been the major concern of many computer science scholars. This paper highlights the development of a biometric fingerprint recognition system using an artificial intelligence method. The methodology used is structured into three main steps: fingerprint image acquisition, feature extraction and comparison or matching. Firstly, we use non-contact fingerprint images for training the recognition model to allow the developed system to work without contact. Secondly, we used a database of nineteen individuals each having fifteen fingerprint images acquired without contact. To perform the transfer learning, we have exploited the MobileNets model while adapting its architecture to the new task of contactless fingerprint classification. After training the new model obtained, we performed it evaluation through a confusion matrix. This evaluation reveals that the developed method confuses one individual out of 19, i.e. a confusion rate of 5.26%. This rate testifies to the efficiency of the method used for non-contact fingerprint recognition.

Keywords: biometrics, recognition Fingerprints, contactless, artificial intelligence, transfer learning,

1. Introduction

The With the evolution of technology and the increasing use of computers in all areas of life, the issue of securing computer systems has become of paramount importance for scientists. Traditional authentication methods such as passwords, or access badges are no longer able to guarantee secured-access to systems that must meet a high level of security [1]. Verifying an individual's identity in order to avoid the risk of fraudulent access to an IT system requires, the use of secure authentication methods. Biometrics has become one of the most important solutions in terms of ensuring computer systems security. Biometrics is a global technique aimed at establishing a person's identity by measuring a morphological (such as the face), biological (such as DNA, genetic heritage) and/or behavioural (such as a signature) feature [2] [3] [4] [5].

Among all biometrics, fingerprints are the most convenient human feature, widely used for the purpose of identifying individuals [6]. Fingerprints have been used in various applications such as forensics, transaction authentication, mobile phone unlocking etc. and are still the most widely used feature in the field of biometrics to authenticate and identify individuals because of their universality and convenience [7]. Most of the proposed algorithms for fingerprint recognition are based on minutiae matching. The main features of fingerprint ridge minutiae are terminal ridges, bifurcations and short ridges [8]. Although many previous works have achieved a high level of accurate performance, they have only focused on preprocessing.

However, in recent years, with the advent and evolution of the possibilities offered by artificial intelligence, some research works have been carried out in various fields to solve previously complicated tasks, through the development of models capable of learning and predicting.

Deep learning has been used for various problems such as classification, segmentation, emotion analysis [9], face recognition [10] and object detection etc. and has significantly improved performance over traditional methods. However, this deep learning method requires the use of very large databases in order to be effective.

There are multiple public databases for fingerprints of reasonable sizes but they are mostly provided with a limited number of images per class (usually less than 20 fingerprint images per person), which then makes training a neural network model from scratch complicated and often even inefficient with these datasets.

To overcome this problem, the transfer learning method of artificial intelligence has been identified as an effective solution.

In this piece of scholarship, we apply this transfer learning method on a relatively small set of fingerprint data, in order to build an artificial intelligence model capable of efficiently recognising individuals through non-contact fingerprints.

 | 10.20533/ijmip.2042.4647.2023.0069

2. Method

2.1. Fundamental theoretical aspects related to the proposed system

We will briefly describe the basic theoretical aspects of the work.

2.1.1. Biometrics. Jain and al [11] have defined biometrics as the science of automatically establishing the identity of an individual based on physiological or behavioural feature. Its purpose is an individual's identification and authentification on the basis of a recognisable and verifiable set of data that is unique and specific to the individual. Biometrics checks the identity of an individual by verifying what the person is and not by using what the person has (key, access card, ...) nor by using what the person knows (password). It is therefore less vulnerable than traditional means of identification [12]. Biometric modalities can be classified into two main categories: pure modalities and soft modalities. The use of one or the other of these two categories depends on the objectives sought in the design of the system.

2.1.2. The fingerprint. The fingerprint is one of the pure modalities in the field of biometrics. The fingerprint is a graphical representation of streamlined ridges and valleys on the surface of human fingers [13]. This representation consists of multiple features that are unique from one individual to another. A good quality fingerprint usually has between 40 and 100 characteristic points [14] [15], but a dozen points are considered sufficient to identify a fingerprint pattern [13]. Fingerprints are immutable and therefore do not change over time (except in the case of an accident such as a burn). Fingerprints are considered unique between individuals, and between fingers of the same person [16].

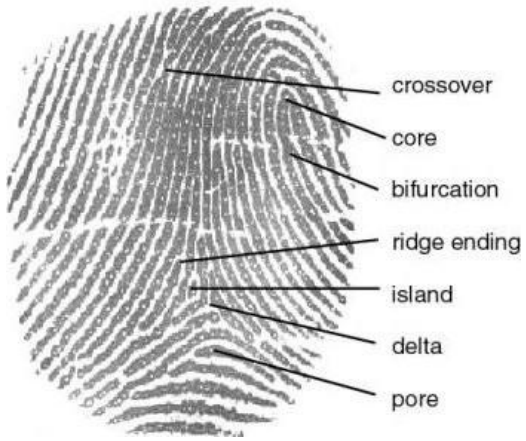

Figure 1. Features present on a fingerprint [6]

Fingerprints are classified according to the Henry system. In this system, the classification is based on the general topography of the fingerprint and allows for the definition of feature. They consist of ridge terminations, the point where the ridge ends, and bifurcations, the point where the ridge splits into two. The core is the inner point, usually in the middle of the print. It is often used as a reference point to locate the other minutes. Other terms are also encountered: lake, island, delta, valley. Figure 1 illustrates these features.

2.1.3. Contactless fingerprint. Most of the current fingerprint-based systems for identifying individuals are contact-based. These systems work with pressure sensors to retrieve fingerprints. Unfortunately, due to some non-linear distortions, such as excessive pressure and twisting of the fingers during enrolment, this process can lead to distortion of details compared to the original [17]. To address this problem, a fingerprint matching method using non-contact images for fingerprint verification can be used. For this purpose, fingerprint images are obtained by using a camera with a good resolution as a sensor under specific conditions.

2.1.4. Transfer learning. Transfer learning is an artificial intelligence learning technique that transfers knowledge gained from solving one task to another related task in order to facilitate learning the new model. This knowledge can take different forms depending on the problem and the data. Thus, in transfer learning, a model trained for one task is reused for another related task, usually by adaptation to that new task [18]. For example, a model that has been trained to recognise bicycles can be easily adapted to learn to recognise motorbikes. The advantage of this method lies in the use of a reduced data size but also in the speed of learning the new model.

2.2. Database and materials. For our system, we use fingerprint images acquired remotely with a camera. The database used contains fifteen images of nineteen individuals, i.e. a total of 285 images. We have obtained these images from the work of Djara et al. [16] who have described the image acquisition process. Djara et al. [2] have developed a non-Contact Biometric Fingerprint Software (CBFS) for the acquisition and processing of our images.

The non-contact fingerprint acquisition system consists of this CBFS to visualise the sharpness of the finger prior to capture, a webcam for digital photo taking, and lighting equipment. The user is asked to place their finger in a fixed position, with the back of their finger in the specified location and their palm facing the camera. A medium resolution webcam (Logitech Pro9000), controlled by an interface as shown in Figure 2 is used to take the images. Figure 3 shows a sample of images from the database.

 | 10.20533/ijmip.2042.4647.2023.0069

To conduct the experiments, we have adopted the Colaboratory platform. This is a cloud service developed by Google that supports machine learning research through the training of machine learning models. All the tools necessary for the development of the models are provided with this service and it is therefore not necessary to carry out any further installation on our computer. Google Colaboratory, more commonly known as "Google Colab" or simply "Colab", is a research project aimed at prototyping machine learning models on powerful Hardware options such as GPUs and TPUs [19].

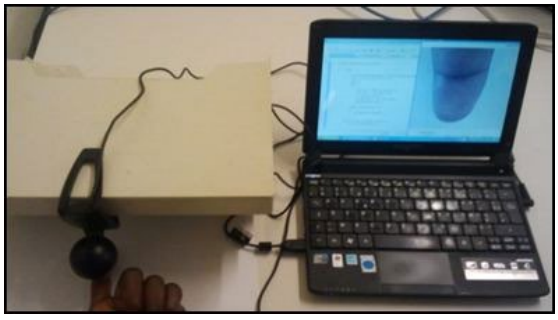

Figure 2. Non-contact fingerprint image acquisition system [16]

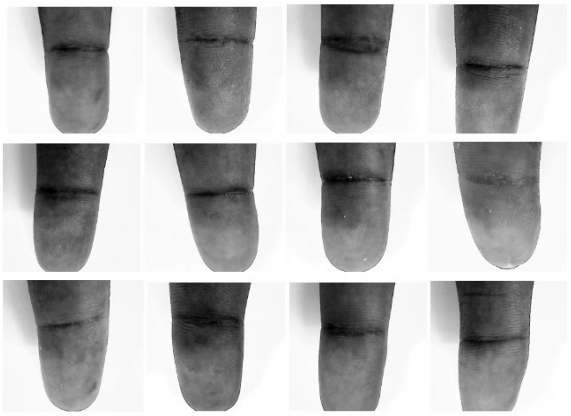

Figure 3. Sample images from the fingerprint database

We worked in the Jupyter NoteBook environment provided directly by Colab. Jupyter Notebook (JN, also known as Ipython Notebook) provides built-in interactive manuals that allow different mathematical models to be built, simulated, verified and tested on these models [20].

2.3. The MobileNet learning model

Complex neural network models based on deep learning [21] have proven to be effective in solving many problems, due to the high accuracies that can be achieved by exploiting them. However, they often require a huge amount of computation and model parameters, which is not suitable for all types of devices (e.g. mobile and embedded). MobileNet was therefore designed to significantly reduce the number of parameters and the computational cost. The main idea of MobileNet is to use a depth-separable convolution. Two hyper parameters, a width multiplier and a resolution multiplier, are used to find a compromise between accuracy and latency [22].

TensorFlow was used to train the MobileNet models using RMSprop [23] with an asynchronous gradient descent similar to that of Inception V3 [24]. Mobile networks can work with many tasks, including object detection, classification, large-scale geolocation, etc.

For the realisation of our authentication system, we have used the first version of MobileNet to perform a learning transfer. The basic architecture of the model is shown in Figure 4.

Type / Stride	Filter Shape	Input Size
Conv / s2	$3 \times 3 \times 3 \times 32$	$224 \times 224 \times 3$
Conv dw / s1	$3 \times 3 \times 32$ dw	$112 \times 112 \times 32$
Conv / s1	$1 \times 1 \times 32 \times 64$	$112 \times 112 \times 32$
Conv dw / s2	$3 \times 3 \times 64$ dw	$112 \times 112 \times 64$
Conv / s1	$1 \times 1 \times 64 \times 128$	$56 \times 56 \times 64$
Conv dw / s1	$3 \times 3 \times 128$ dw	$56 \times 56 \times 128$
Conv / s1	$1 \times 1 \times 128 \times 128$	$56 \times 56 \times 128$
Conv dw / s2	$3 \times 3 \times 128$ dw	$56 \times 56 \times 128$
Conv / s1	$1 \times 1 \times 128 \times 256$	$28 \times 28 \times 128$
Conv dw / s1	$3 \times 3 \times 256$ dw	$28 \times 28 \times 256$
Conv / s1	$1 \times 1 \times 256 \times 256$	$28 \times 28 \times 256$
Conv dw / s2	$3 \times 3 \times 256$ dw	$28 \times 28 \times 256$
Conv / s1	$1 \times 1 \times 256 \times 512$	$14 \times 14 \times 256$
$5\times$ Conv dw / s1	$3 \times 3 \times 512$ dw	$14 \times 14 \times 512$
$5\times$ Conv / s1	$1 \times 1 \times 512 \times 512$	$14 \times 14 \times 512$
Conv dw / s2	$3 \times 3 \times 512$ dw	$14 \times 14 \times 512$
Conv / s1	$1 \times 1 \times 512 \times 1024$	$7 \times 7 \times 512$
Conv dw / s2	$3 \times 3 \times 1024$ dw	$7 \times 7 \times 1024$
Conv / s1	$1 \times 1 \times 1024 \times 1024$	$7 \times 7 \times 1024$
Avg Pool / s1	Pool 7×7	$7 \times 7 \times 1024$
FC / s1	1024×1000	$1 \times 1 \times 1024$
Softmax / s1	Classifier	$1 \times 1 \times 1000$

Figure 4. MobileNet architecture [22]

2.4. Adapting the model

The architecture presented in the previous Fig shows that the MobileNets model has 1000 output classes. In our case we have 19 individuals to classify. We have then removed the last layer for our adaptation while keeping the model parameters and the other layers. Then, we have added two new dense layers of 1024 neurons and a dense layer of 512 neurons with Relu as the activation function. These layers will actually allow our new model to learn more complex functions.

A final output layer of 19 neurons with the Sotfmax activation function was completed to determine the classification probabilities of each class. Our fingerprint authentication system is essentially composed of three basic steps, which are:

 | 10.20533/ijmip.2042.4647.2023.0069

pre-processing, analysis or feature extraction by an artificial neural network and comparison or matching.

2.5. Pre-treatment

Before we can use our images to train our model, it is necessary to do some preprocessing on these images to enable the model to process them. The preprocessing step consists of resizing the images to the same size so that they can be used in the training model. Thus, all the images were resized to a format of 300X300 pixels.

2.6. Extraction of feature

In recent years, the evolution of artificial intelligence has made it possible to solve

many problems in various fields. Deep Learning [9] is used today to solve various problems such as classification, segmentation, image subtitling [25], emotion analysis [26], face recognition and object detection [27], and has significantly improved performance compared to traditional approaches [18]. Thus, convolutional neural networks (CNNs) [28] have been very successful in various fields of computer vision and natural language processing.

In the field of biometrics, most of the proposed algorithms for fingerprint recognition are based on minutiae matching. However, with artificial intelligence, the focus has been on developing neural network models to learn fingerprint features for prediction. In this direction, we can mention for example Minaee et al. [28] who proposed a fingerprint recognition using multi-layer convolutional diffusion networks.

For our fingerprint recognition system, we have opted for a transfer learning method. Indeed, the knowledge acquired by a neural network for a task can be transferred to another neural network to solve a similar problem: this is called Transfer Learning. In transfer learning, a model trained for one task is readapted to another related task, usually by some adaptation to the new task. This method has several advantages over direct learning methods, including the use of a reduced size of training data and better generalization of the training model. Most of the time, training a model from scratch is very labor intensive and requires a lot of data. With Transfer Learning, we can use less training data to get good results. Models that have been trained using Transfer Learning are also better able to generalize from one task to another because they have been trained to learn to identify features that can be applied to new contexts. For our case, we have used the MobileNet model architecture [29].

Figure 5 shows that it obviously appears that in a reduced number of iterations, our system manages to correctly validate the training of the model. The transfer learning method therefore has the advantage of rapid convergence and learning.

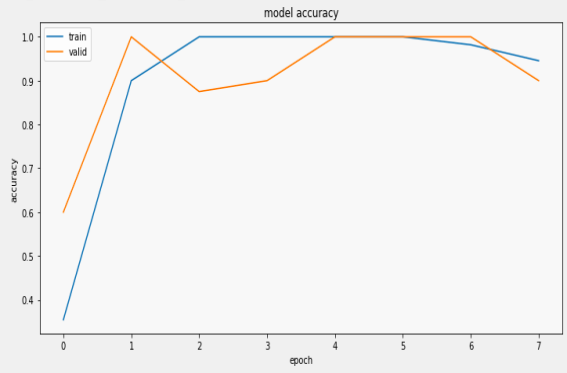

Figure 5. Learning curve of the fingerprint recognition model

2.7. Comparison or matching

At this stage, we make predictions about the classification of individuals. Each individual in the database is represented by a class. This step allows us to check whether the fingerprint of an individual corresponds to it. Once the recognition system has been trained with the fingerprint images, it is presented with other unknown images to see if the system can match them to the correct individuals. Our recognition system works and allows us to accurately identify any individual's identity.

3. Results and Discussion

To evaluate the performance of the fingerprint classification system, we have opted for the construction of the confusion matrix. This is a matrix that allows us to quickly measure the quality of a classification system. In this matrix, each row corresponds to a real class, each column corresponds to an estimated class. Thus, at the level of each cell, row A, column B contains the number of elements of real class A that have been estimated as belonging to class A. With this matrix we can easily determine whether the system correctly classifies the different classes. This confusion matrix will allow us to summarize the classification performance of our model. Here, it is a table of 19 different combinations between the expected prediction values and those obtained. Figure 6 shows the matrix obtained. We can see that apart from individual 7 who can be confused with individual 3, all other individuals are correctly identified without any confusion in their identification. The transfer learning method was thus effective for the recognition of fingerprint images.

The recognition of fingerprint images has been done using artificial intelligence. The transfer learning method has been used. It has the advantage

 | 10.20533/ijmip.2042.4647.2023.0069

of being quick to implement thanks to the use of a small amount of data and the rapid learning of pre-trained models on large databases. This method allowed us to implement a biometric authentication system using fingerprints acquired without contact with the sensor. Its efficiency was proven thanks to the confusion matrix obtained. On the other hand, the approximately small number of individuals in the database could be the source of this efficiency in the classification of fingerprint images. It would be interesting to increase the number of individuals present in the database to see their effect on the efficiency of the fingerprint recognition method by transfer learning.

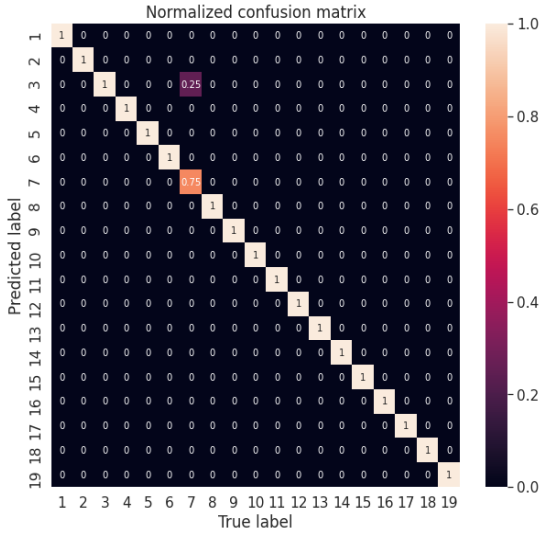

Figure 6. Model confusion matrix

4. Conclusion

The system we have proposed in this paper satisfies the requirements we wanted to achieve at the beginning of this work. Our objective was to realize a biometric fingerprint authentication system using images acquired without contact while adopting the artificial intelligence method of transfer learning.

The first step was the acquisition of non-contact fingerprint images. However, we exploited an already directly available database. Then we have made an adaptation of the MobileNets model in order to create a new model capable of learning using the old parameters of the original model. After evaluating the results, we can say that this transfer learning method is effective for the identification of fingerprint images.

5. References

[1] Y. Safaa El-Din, M. N. Moustafa, et H. Mahdi, « Deep convolutional neural networks for face and iris presentation attack detection: survey and case study », IET Biom., vol. 9, no 5, p. 179-193, sept. 2020, DOI: 10.1049/iet-bmt.2020.0004.

[2] T. Djara, A.-A. Sobabe, M. Agbomahena, et A. Vianou, « Practical Method for Evaluating the Performance of a Biometric Algorithm: Second EAI International Conference, AFRICATEK 2018, Cotonou, Benin, May 29–30, 2018, Proceedings », 2019, p. 125-132. DOI: 10.1007/978-3-030-05198-3_11.

[3] A. K. Jain, A. A. Ross, et K. Nandakumar, Introduction to Biometrics. Boston, MA: Springer US, 2011. DOI: 10.1007/978-0-387-77326-1.

[4] F. Jan, M. I. B. Ahmed, et N. Min-Allah, « Databases for Iris Biometric Systems: A Survey », SN Comput. Sci., vol. 1, no 6, p. 324, Nov. 2020, DOI: 10.1007/s42979-020-00344-3.

[5] S. Ayeswarya et J. Norman, « A survey on different continuous authentication systems », Int. J. Biom., vol. 11, no 1, p. 67, 2019, DOI: 10.1504/IJBM.2019.096574.

[6] K. Prihodova et M. Hub, Biometric Privacy through Hand Geometry- A Survey, in 2019 International Conference on Information and Digital Technologies (IDT), Zilina, Slovakia: IEEE, juin 2019, p. 395-401. DOI: 10.1109/DT.2019.8813660.

[7] The biometrics market. https://www.biometrie-online.net/biometrie/le-marche (consulté le 24 octobre 2022).

[8] A.-A. Sobabe Ali Tahirou et al., « Authentification par la biométrie multimodale sans contact »: Thesis, EPAC/UAC, 2021. Consulté le: 26 octobre 2022. [En ligne]. Disponible sur: http://biblionumeric.epac-uac.org:8080/jspui/handle/123456789/2845.

[9] T. Djara, A. M. Ousmane, et A. Vianou, « Emotional State Recognition Using Facial Expression, Voice, and Physiological Signal » :, Int. J. Robot. Appl. Technol., vol. 6, no 1, p. 1-20, janv. 2018, DOI: 10.4018/IJRAT.2018010101.

[10] Y. Kortli, M. Jridi, A. Al Falou, et M. Atri, « Face Recognition Systems: A Survey », Sensors, vol. 20, no 2, p. 342, janv. 2020, DOI: 10.3390/s20020342.

[11] A. Jain, P. Flynn, et A. Ross, Handbook of Biometrics. 2008. DOI: 10.1007/978-0-387-71041-9.

[12] M. Lemmouchi, Reconnaissance Biométrique par Fusion Multimodale », doctoral, Université de Batna 2, 2020. Consulté le: 26 octobre 2022. [En ligne]. Disponible sur: http://eprints.univ-batna2.dz/1866/

[13] T. Borah, K. Sarma, et P. Talukdar. Fingerprint Recognition Using Artificial Neural Network. Int. J. Electron. Signals Syst., vol. 3, no 1, août 2020, DOI: 10.47893/IJESS.2013.1140.

[14] Biometric System Vulnerabilities: A Typology of Metadata. ASTES Journal. https://www.astesj.com/v05/i01/p25/ (consulté le 26 octobre 2022).

[15] H. Nabil, « Méthode hybride en biométrie: Application à la paume de la main & l'Oreille », Thesis, 2017. Consulté

le: 26 octobre 2022. [En ligne]. Disponible sur: http://dspace.univ-guelma.dz/ jspui/handle/123456789/116

[16] T. Djara, M. Assogba, A. Naït-ali, et A. Vianou, Registration of fingerprint images in contactless biometrics. Journée de la Recherche Scientifique de l'Université de Lomé, Togo, p. 133-145, juillet 2013.

[17] T. Djara, M. K. Assogba, et A. Vianou, « A Contactless Fingerprint Verification Method using a Minutiae Matching Technique », Int. J. Comput. Vis. Image Process., vol. 6, no 1, p. 12-27, janv. 2016, DOI: 10.4018/IJCVIP.2016010102.

[18] S. Albawi, T. A. Mohammed, et S. Al-Zawi, « Understanding of a convolutional neural network », in 2017 International Conference on Engineering and Technology (ICET), Antalya: IEEE, août 2017, p. 1-6. DOI: 10.1109/ICEngTechnol.2017.8308186.

[19] E. Bisong, Building Machine Learning and Deep Learning Models on Google Cloud Platform: A Comprehensive Guide for Beginners. Berkeley, CA: Apress, 2019. DOI: 10.1007/978-1-4842-4470-8.

[20] C. R. Maestre, F. A. Gregori, M. P. López, et R. R. Aldeguer, Jupyter Notebook: Theory And Practice Of Mathematical Models in Engineering and Architecture. ICERI2016 Proc, p. 6523-6530, 2016, DOI: 10.211 25/iceri.2016.0492.

[21] B. B. Benuwa, Y. Z. Zhan, B. Ghansah, D. K. Wornyo, et F. Banaseka Kataka, « A Review of Deep Machine Learning », Int. J. Eng. Res. Afr., vol. 24, p. 124-136, juin 2016, DOI: 10.4028/www.scientific. net/JERA.24.124.

[22] A. G. Howard et al., MobileNets: Efficient Convolutional Neural Networks for Mobile Vision Applications, CoRR, vol. abs/1704.04861, 2017. Consulté le: 25 octobre 2022. [En ligne]. Disponible sur: http://arxiv.org/abs/1704.04861.

[23] T. Tieleman et G. Hinton, Lecture 6.5-rmsprop: Divide the gradient by a running average of its recent magnitude, COURSERA Neural Netw. Mach. Learn., vol. 4, no 2, p. 26-31, 2012.

[24] C. Szegedy, V. Vanhoucke, S. Ioffe, J. Shlens, et Z. Wojna, Rethinking the Inception Architecture for Computer Vision, in 2016 IEEE Conference on Computer Vision and Pattern Recognition (CVPR), Las Vegas, NV, USA: IEEE, juin 2016, p. 2818-2826. DOI: 10.1109/CVPR.2016.308.

[25] M. Cho, T. Kim, I.-J. Kim, K. Lee, et S. Lee, « Relational Deep Feature Learning for Heterogeneous Face Recognition », IEEE Trans. Inf. Forensics Secur., vol. 16, p. 376-388, 2021, DOI: 10.1109/TIFS. 2020.3013186.

[26] A. Krizhevsky, I. Sutskever, et G. E. Hinton, « ImageNet classification with deep convolutional neural networks », Commun. ACM, vol. 60, no 6, p. 84-90, mai 2017. DOI: 10.1145/3065386.

[27] G. Guo et N. Zhang, « A survey on deep learning based face recognition », Comput. Vis. Image Underst., vol. 189, p. 102805, déc. 2019, DOI: 10.1016/j.cviu.2019.102805.

[28] S. Minaee, E. Azimi, et A. Abdolrashidi, FingerNet: Pushing The Limits of Fingerprint Recognition Using Convolutional Neural Network, juill. 2019. Consulté le: 25 octobre 2022. [En ligne]. Disponible sur: https://ui.adsabs.harvard.edu/abs/20 19arXiv190712956M.

[29] Md. R. Islam, N. Tasnim, et S. B. Shuvo, « MobileNet Model for Classifying Local Birds of Bangladesh from Image Content Using Convolutional Neural Network, in 2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT), Kanpur, India: IEEE, juill. 2019, p. 1-4. DOI: 10.1109/ICCCNT456 70.2019.8944403.

